AKKODIS

Moving Target

How Growth and Urgency are Reshaping the Defense Sector

AKKODIS

Content

In most parts of the world, countries are reconsidering their place in the global network of alliances and partnerships. Reacting to new geopolitical uncertainty and a changing security environment, they are rethinking their military readiness and security posture.

This geopolitical shift is changing the military industrial complex, both nationally and regionally.

Three challenges are reshaping the defense sector: growth, urgency, and technology. How defense OEM's–including their eco-system of partners, suppliers, contractors and start-ups–react to these challenges, will determine their fate in the market.

Examining the three challenges, this e-book points to both concrete case stories as well as conceptual rethinking, to meet the emerging new reality of defense R&D and manufacturing:

The pressure to deliver fast will lead to new partnerships and constellations, with well-established defense manufacturers taking on new roles, Tier 2 and Tier 3 suppliers gaining importance, and newcomers contributing with expertise from the civilian sector.

While firepower remains crucial, the power of data, information and communication is increasing. Everything–soldiers, equipment etc.–is becoming even more connected. Situational awareness is essential, and on the battlefield, nothing is more important than the military's nervous system C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance).

Flexibility and interoperability are key as well. Just as one of the hallmarks of great militaries is the ability to adapt to changing conditions, defense equipment and solutions must be able to integrate easily into new battlefield concepts and technological platforms.

While navigating geopolitical change, the defense sector is integrating technological advancements, driven by data, sensors, computing power and an increased focus on interoperability. The new reality of defense R&D and manufacturing is complex and challenging, defined by a strong sense of urgency. Now is the time to do better, faster.

01
Challenging Established Structures in Defense Innovation & Manufacturing

Typically, countries have their own defense industry, characterized by large, well-established companies. These companies have a long track record of manufacturing equipment for their domestic market and for export.

Compared to new entrants these incumbents have a unique position, drawing on deep technical knowledge of the domain, strong customer relations and detailed understanding of how equipment and solutions are used in the field. Moreover, they have secure physical and digital infrastructure in place, and knowledge of existing legacy platforms that must be integrated into new systems.

Incumbents are Adapting

The size, experience and market position of this defense industrial base makes it indis-pensable. How are these established players reacting to the emerging new reality of defense R&D and manufacturing, with its emphasis on volume, urgency and flexibility?

Firstly, they are increasing their activity, adding new assembly lines to existing ones and boosting output as much as possible.

Secondly, their role in the ecosystem is changing. Internal expansion in Tier1-companies will not be enough to handle the steep rise in demand over the coming years. The influx of investment will lead to structural change, with manufacturers, contractors, consultancies and startups creating new value chains and develop-ing new ways of collaborating and partnering.

According to the NATO Secretary General's Annual Report for 2024, published 24 April 2025, the previ-ous year's 19.4% increase in defense spending is far from enough. A "quantum leap" is required to strengthen NATO's "collective deterrence and de-fense posture", and national defense investment must increase to between 3.5 and 3.7 % of GDP.

With the defense market growing at a high pace, Tier 2 and Tier 3 suppliers will experience a change in their role as well. They will continue to provide their expertise as subcontractors to the big "gatekeepers" of the sector. But at the same time, their workload will increase. They will be trusted with larger parts of a system, because, to meet customer demand, the big defense man-ufacturers will favor partners willing and able to deliver on more than just narrow slices of a system or a project.

Newcomers and New Constellations

Tier 2 and Tier 3 suppliers can be well-established defense actors or newcomers to the sector. They can be small, agile startups or big commercial technology companies adapting their products to defense requirements. What they have in common is business models and development cycles typically faster and shorter than the average defense company, often utiliz-ing cutting edge digital technologies.

These competencies fit well with the demand for faster development and manufacturing. Together they will encourage new ways of developing and designing defense solutions. There will be a gradient towards more use of off-the-shelf products and solutions, combining them and ruggedizing them to fit the strict requirements of the defense domain, as well as finding ways to integrate diverse solutions into a network of systems, designed for interoperabili-ty and flexibility.

Boosting Manufacturing Efficiency

It goes to reason that the steep increase in defense industry output will influence manufacturing as well. Due to strict regulations and high security standards, defense manufacturers in general, work with longer development and product life cycles than the average producer of consumer products. As in many other industries, this creates potential for leveraging Industry 4.0 processes, to optimize production, quality control and flexibility.

The fact that many of the newcomers to the defense domain are fluent in digital technologies and advanced electronics, stands to benefit the industry greatly. Their capabilities can be integrated into defense products, as well as utilized to optimize production. Many of the new contributors originate from more industrial sectors with a higher pace of innovation, for instance automotive and consumer electronics. Due to faster turnover, these sectors have come further in implementing advanced manufacturing technologies and can serve as catalysts for Industry 4.0 implementations in defense.

Securing Supply Chain Sovereignty

Driven by the rise in geopolitical tensions and the weaponization of trade links, supply chains have come into sharper focus.Supply chain safety and efficiency is crucial, and that includes everything from sourcing critical materials to ensuring the required quality and timely delivery of parts and components.

Re-localization is becoming even more important, not only due to the changing security landscape, but also because of rising costs of shipping and disturbances in international shipping routes. All this leads to a heightened focus on the integrity of defense sector supply lines.

While re-localization is a priority, it comes with added cost. High-cost countries will feel an added pressure to consider, which parts of a defense product or system must be produced at home and which parts could safely be labelled low-risk and thus sourced from low-cost friends and allies.

Exploring New Ways of Working

The push for faster development cycles, together with the rising complexity of defense equipment, and the growing importance of its digital components, is necessitating new ways of working. Process Automation, DevOps, Artificial Intelligence – new tools are being adapted to the defense domain.

Also, the Model Based Systems Engineering approach is creating huge benefits in complex development projects. Compared to traditional, document-based methods, it ensures that by leveraging digital models, all participants work with the same information and allows for potential issues to be identified at an early stage.

Just as MBSE is answering the challenge of increasingly complex products and solutions, the concept of System of Systems Engineering is gathering momentum as well: Modern net-centric warfare places new demands on the components of the military network and on the network's ability to integrate new components easily, efficiently and securely.

System of Systems Engineering

One result of this evolution in engineering thinking is the development of an approach known as System of Systems Engineering—a term first coined in the 1950s and later advanced through American defense research beginning in the 1980s.

System of Systems Engineering is a subfield of Systems Engineering that focuses on the boundaries and interactions between independent systems, designing them to collectively fulfill the requirements of a larger, overarching system.

The term describes a system composed of independent systems interact-ing jointly towards a common goal. Examples of such collaborating sys-tems can be seen in air traffic management, emergency medical response, or energy infrastructure.

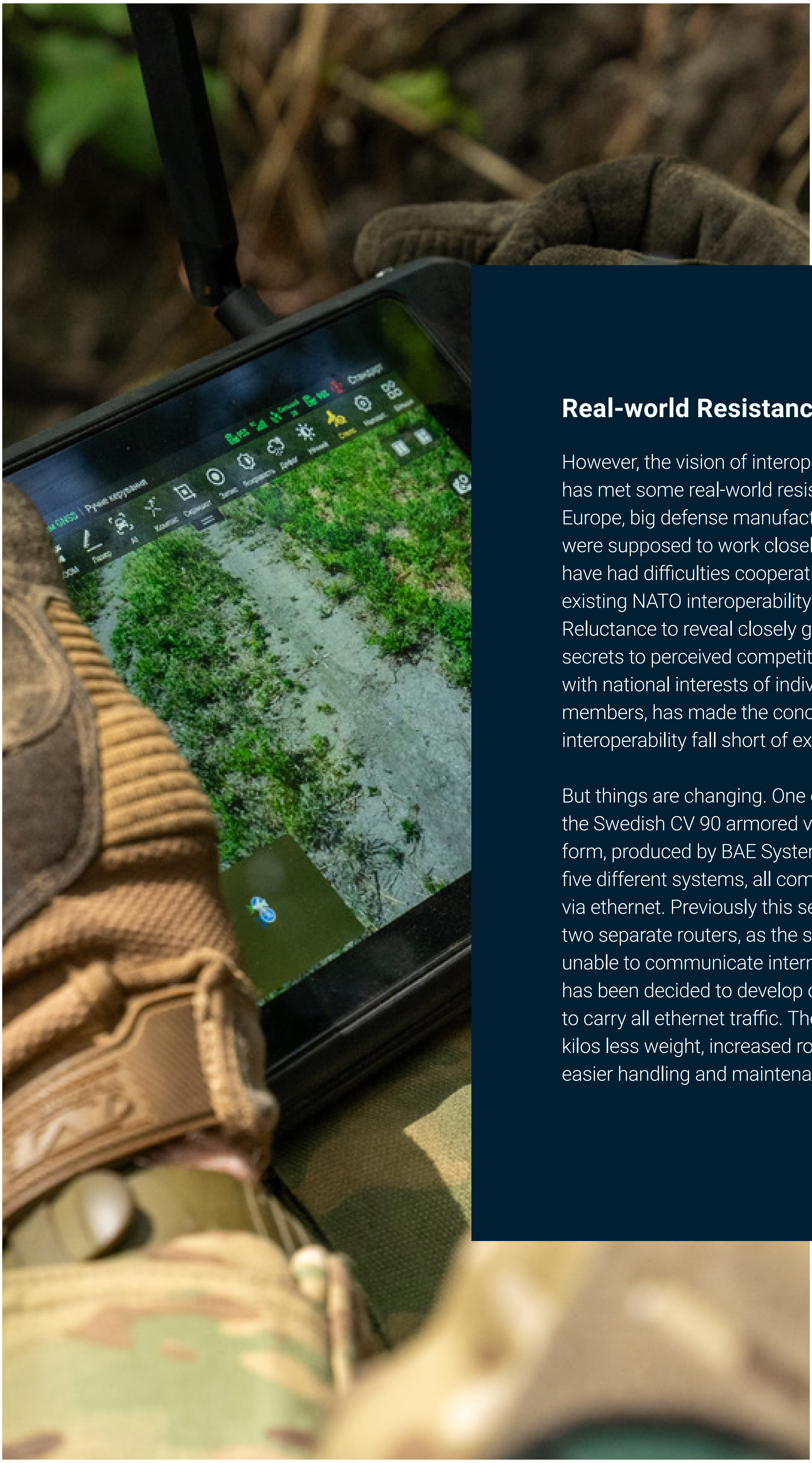
Many of the subsystems working in these types of interlinked systems will have existed before, but often with communication gaps between them. Now, advances in network and communication technology have made it possible for them to become unified and work closely together.

In a defense setting, fire control can highlight the strengths of a System of Systems ap-proach. To point out targets and to speed up the OODA loop (observe, orient, decide, act), artillery systems can benefit from information coming from drones, apps, sensors, civilians sending SMS messages etc. All this informa-tion must be integrated, validated and used for decision making. As the war in Ukraine is showing, there is a clear advantage in having systems that are built for flexibility and able to integrate new sources -of information and to adapt to changing conditions on the battlefield.

A large-scale example of System of Systems Engineering is the European FCAS (Future Combat Air System). A new generation of piloted fighter jets will work together with drones, and connected to other weapon systems on the ground, at sea, in space and in cyberspace via a Combat Cloud. This system of systems is designed for easy inclusion of future technologies and weapon systems, enabling collaborative combat across domains.

Mine-hunting

Akkodis is currently working on new mine-hunting solutions incorporating both air, surface and below-surface drones. A mine-hunting vessel will launch several surface drones to establish an overview of the mine field ahead. These surface drones can launch underwater drones to scan suspicious objects, working together with airborne drones. Sophisticated data links between this network of drones allow for autonomy and AI-powered decision-making in neutralizing the mine field. The challenge in this type of system of systems is not only to build different types of drones. It is also to perform efficient mission planning, and to secure precise drone navigation and reliable decision-making capabilities.



Real-world Resistance

However, the vision of interoperability has met some real-world resistance. In Europe, big defense manufacturers that were supposed to work closely together, have had difficulties cooperating, despite existing NATO interoperability standards. Reluctance to reveal closely guarded trade secrets to perceived competitors, combined with national interests of individual EU members, has made the concept of interoperability fall short of expectations.

But things are changing. One example is the Swedish CV 90 armored vehicle platform, produced by BAE Systems. It has five different systems, all communicating via ethernet. Previously this setup required two separate routers, as the systems were unable to communicate internally. Now, it has been decided to develop one system to carry all ethernet traffic. The result? 21 kilos less weight, increased robustness and easier handling and maintenance.

Updating Legacy Equipment

The concepts of The Connected Soldier and The Internet of Military Things are based on connectedness and situational awareness. They come with an increased focus on innovation and agility, and the defense sector is gradually embracing new develop-ment methods to increase efficiency, adapt to change and reduce time-to-frontline.

A special feature of defense tech is the fact, that innovation isn't only about looking into the future but also into the past. Innovative approaches can have a huge impact on existing equipment as well, as boosting defense capabilities is not only about developing new products. It is just as important to minimize downtime and extend the service life of existing equipment by properly maintaining it and updating it to function together with new systems. And in the world of military hardware, equipment has a much longer life span than in the commercial, civilian domain. Therefore, it makes good sense to build software able to run on older hardware or upgrading ageing equipment with communication technology to connect it to the network.

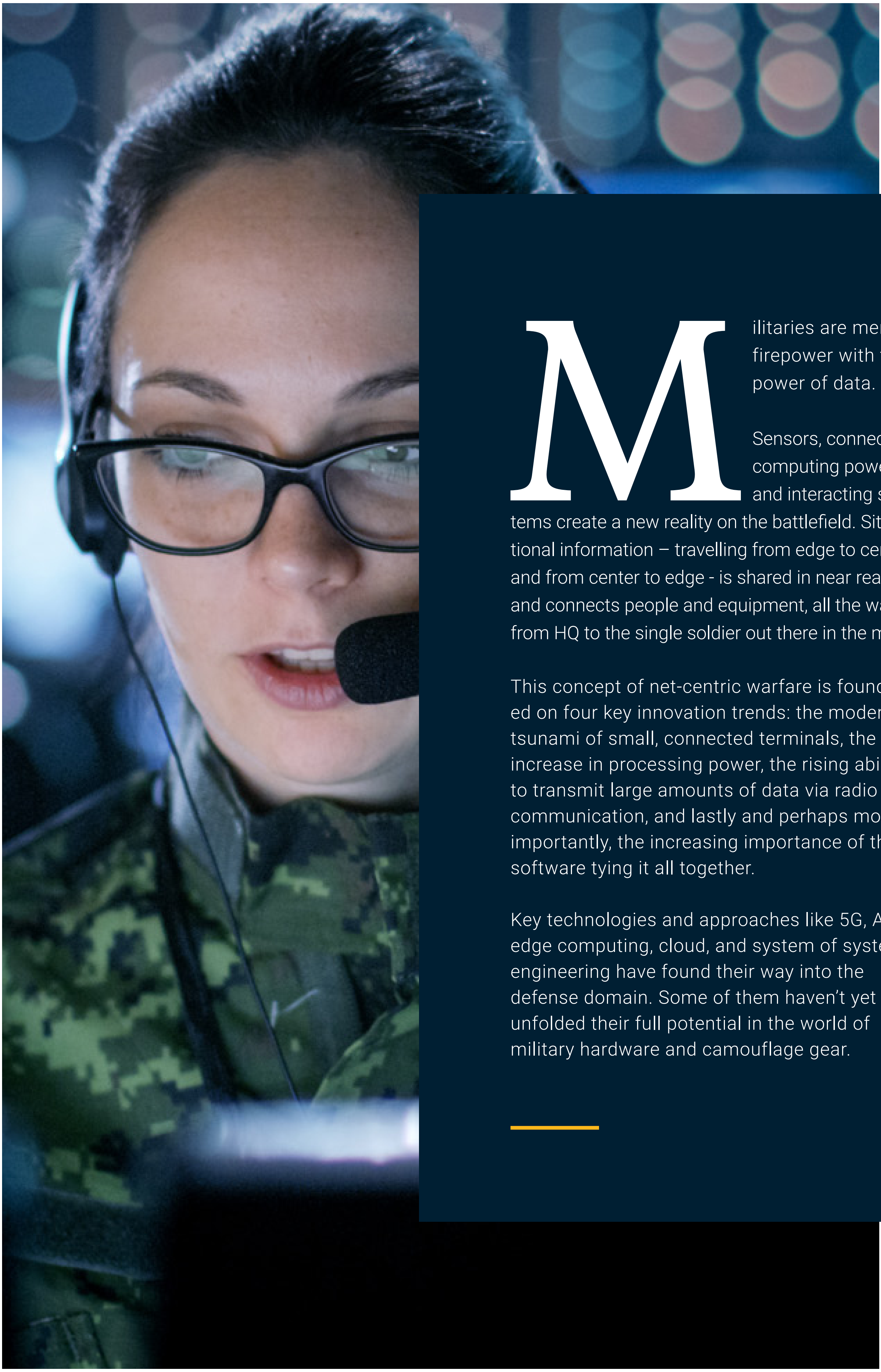
Digital technologies are helping to optimize this attention to legacy equipment and systems. Sensors can provide vital information regarding their condition and facilitate the setup of condition based and predictive maintenance schedules. This can also optimize capacity planning and inventory management, with a more precise overview over which parts are needed when and where.

Control & Display Unit

Akkodis is working on the complete design and development of the next generation Control and Display Unit (CDU), which is the operator station in the new observation and target acquisition system (OTAS) for the German and Dutch army Fennek II reconnaissance vehicles. The OTAS consists of a camera suite for differ-ent conditions and lasers for range measure-ment and target designation, all mounted on a telescopic mast. The CDU has been developed with sustainability in mind, and the new design reduces the environmental footprint, increases the repairability and lifetime significantly, and provides a new standard for soldier safety.

02

Defense Tech Boost: Merging Firepower with Data Power



Militaries are merging firepower with the power of data.

Sensors, connectivity, computing power and interacting systems create a new reality on the battlefield. Situational information – travelling from edge to center and from center to edge - is shared in near real-time and connects people and equipment, all the way from HQ to the single soldier out there in the mud.

This concept of net-centric warfare is founded on four key innovation trends: the modern tsunami of small, connected terminals, the vast increase in processing power, the rising ability to transmit large amounts of data via radio communication, and lastly and perhaps most importantly, the increasing importance of the software tying it all together.

Key technologies and approaches like 5G, AI, edge computing, cloud, and system of systems engineering have found their way into the defense domain. Some of them haven't yet unfolded their full potential in the world of military hardware and camouflage gear.

AI in Action

Artificial Intelligence (AI) is quickly gaining traction in defense, It is no longer just a laboratory curiosity or a technology for headquarters analysis. Edge AI, artificial intelligence deployed at the tactical level, on platforms and systems operating in the field, is already changing the game.

One out of many AI applications operational today is the filtering of massive surveillance streams to identify what matters. Large amounts of drone-generated video imagery is crunched by IA systems, detecting anomalies, identifying potential threats and directing human attention.

This allows for faster and more precise target identification and prioritization. AI systems can now distinguish military vehicles from civilian ones, identify weapon systems, and assess threat levels—all in near-real time.

In the area of jammer detection and electronic warfare support. AI can identify hostile electronic emissions, help locate their sources, and support countermeasures far faster than human operators.

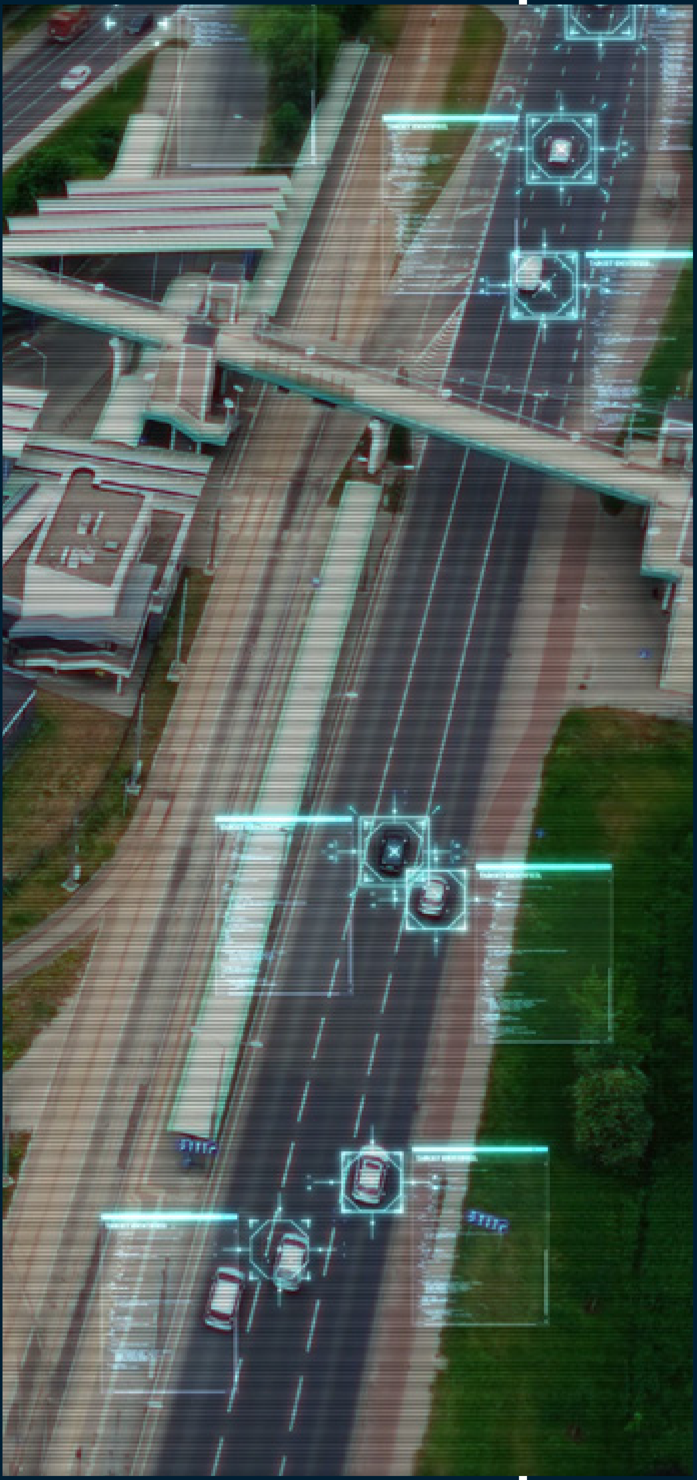
And AI can help commanders perform predivctive threat analysis by pointing to suspicious data patterns that suggest imminent attacks or hostile movement, giving commanders precious additional minutes or hours to respond.

Looking at the ongoing war in Ukraine, AI is integrated deeply into defense tech innovation. Ukrainian firms use curated military datasets for continuous AI training, enabling weekly iteration cycles even amid conflict. Furthermore, the Ukrainian defense industry now develops standalone AI modules that can be integrated into drones, UGVs, or turrets, boosting battlefield autonomy through interoperability.

Data Quality Crucial

The question asked by many military commanders, and by civilian CEOs as well, is how AI can be harnessed for faster and more precise decision making in their specific field.

The answer to that question is by no means short and crystal clear, except for one thing: AI will fail, if the data it crunches is not clean and well structured. Therefore, the starting point of any discussion about AI is data quality. At least 80 % of all work in an AI project goes into data qualification and preparation.



The Akkodis AI-Core Platform

AI-Core merges innovative AI models and conventional, rules-based algorithms into one platform for high-value output. Flexible plug-ins allow for a wide range of use cases, and AI-Core runs on local laptops and desktops, as well as on embedded hardware without internet access and via the cloud.

Early warning: Drones and other potential threats are detected and identified in real-time, optimizing response capacity and safety. AI-powered image analysis identifies incoming objects, even with poor visibility and inferior video imagery. Drones, as well as movement on the ground can be detected, using both video, thermal and RGB cameras.

Battlefield 5G

Similar to AI, 5G is a technological enabler redefining the battlefield. 5G's speed of 10 gigabits per second is estimated to be 100 times faster than 4G. This means that the military can react to emergency situations and control drones and vessels, individually or in swarms, in real-time via the mobile network —and get the most out of artificial intelligence and virtual/advanced reality.

The use of 5G as an operative channel for data transport has come a long way in some militaries. With the help of Software-Defined Networking and Network Function Virtualization it is possible to assign private, specially adapted user areas—so-called "network slices".

This allows the military to establish its own, dedicated and protected 5G communications channels. Norway is one of the frontrunners. Soon existing 4G tactical communication nodes, mounted in every combat vehicle in the Norwegian army, will be upgraded to 5G. Next in line are new mobile base stations and range extenders, to provide powerful and flexible high-speed low-latency communication infrastructure supporting soldiers in the field.

Edge Computing and Combat Cloud

Military 5G will accelerate the utilization of edge computing—whether AI or not—in combat settings. It can be the more traditional version of edge computing, with large amounts of data coming from sensors at the edge being fed into a data center or cloud system, or it can be bringing not only sensors but also computing power to the edge, to reduce data transfer and processing time. Database and signal processing is moving towards the edge, and the equipment making it possible will largely consist of existing products developed initially for other domains adapted to military environments.

This allows for a differentiation of the concept of Combat Cloud. The idea of a centralized Combat Cloud covering a whole region, for instance, will be supplemented with local clouds, placed on different levels of the command structure. To reduce the distance between center and edge, and to secure flexible and fast data communication, there will be differentiated, multi-level combat clouds for various forces out in the field.

Communication Nodes for Military Use

Akkodis produces a range of rugged portable and vehicle mounted nodes for tactical communication. They include the functionality of commercial routers, supporting fixed and mobile communications, including 4G/LTE/5G and mobile ad hoc networks (MANET). They meet the MIL-STD standard for durability and offer optional features such as WiFi and power supply to ensure reliable connectivity in different environments. The nodes also allow for mounting of 3rd party Crypto Modules.

Cybersecurity: Connectedness Equals Risk

The degree of connectedness required for seamless operation within the Internet of Military Things presupposes the firmest possible grip on cyber security.

With the emergence of IoMT, cyber security has become more important than ever. It even seems as if modern interconnectedness is blurring the lines between war and peace. Both below and above the threshold of war, the cyber domain is a battlefield, and always active. Or as NATO puts it in a recent threat assessment report: “Cyberspace is contested at all times”.

Needless to say, militaries require the strictest cyber security measures. The trend towards “net-centric warfare” and the vulnerabilities coming with it, calls for the strongest possible focus on the cyber domain.

Command & Control systems rely heavily on data and intelligence from sensors, radars, satellites, drones etc. Also, the share of networked components in weaponry is steadily increasing. If not all network components are sufficiently cyber-hardened, and the advantages of networking are not properly protected, vulnerabilities appear and whole systems can be compromised.

Cyber security - “Offensive Defense”

To prevent attacks and expose the methods of attackers, Akkodis has developed “Offensive Defense” concepts to counteract cyber-attacks by deploying “honeypots” in the cloud. Honeypots are servers that mimic vulnerable services to attract viruses. They monitor all interactions from an attacker, and once these are collected, data visualization techniques are used to get more insights and sometimes even allow the organization to prevent attacks that have not yet happened. The collected data contains valuable information, such as the top attacking countries or IP addresses, the most-used passwords for attempted attacks, a world map of the attacks, number of attacks per protocol and much more.

Cybersecurity at the Edge

Cybersecurity at the tactical edge is a critical aspect of modern warfare deserving special attention. It goes beyond protecting headquarters networks or strategic assets, though those remain important. It's about the cybersecurity of the systems soldiers depend on in combat.

And the threats are becoming more severe and complex:

The attack surface is expanding exponentially. Every sensor, communication device, weapon system, and vehicle with digital components represents a potential vulnerability. Soldiers now carry more computing power than entire military units had twenty years ago. Each of those devices is a potential target.

As a consequence, the time between vulnerability discovery and exploitation is shrinking. What used to take months now happens in days or hours. Zero-day exploits - vulnerabilities unknown to defenders - are being weaponized at unprecedented rates.

Moreover, adversaries are specifically targeting tactical systems. They recognize that compromising a targeting system, communications network, or logistics platform at a critical moment could be more valuable than breaching a strategic database.

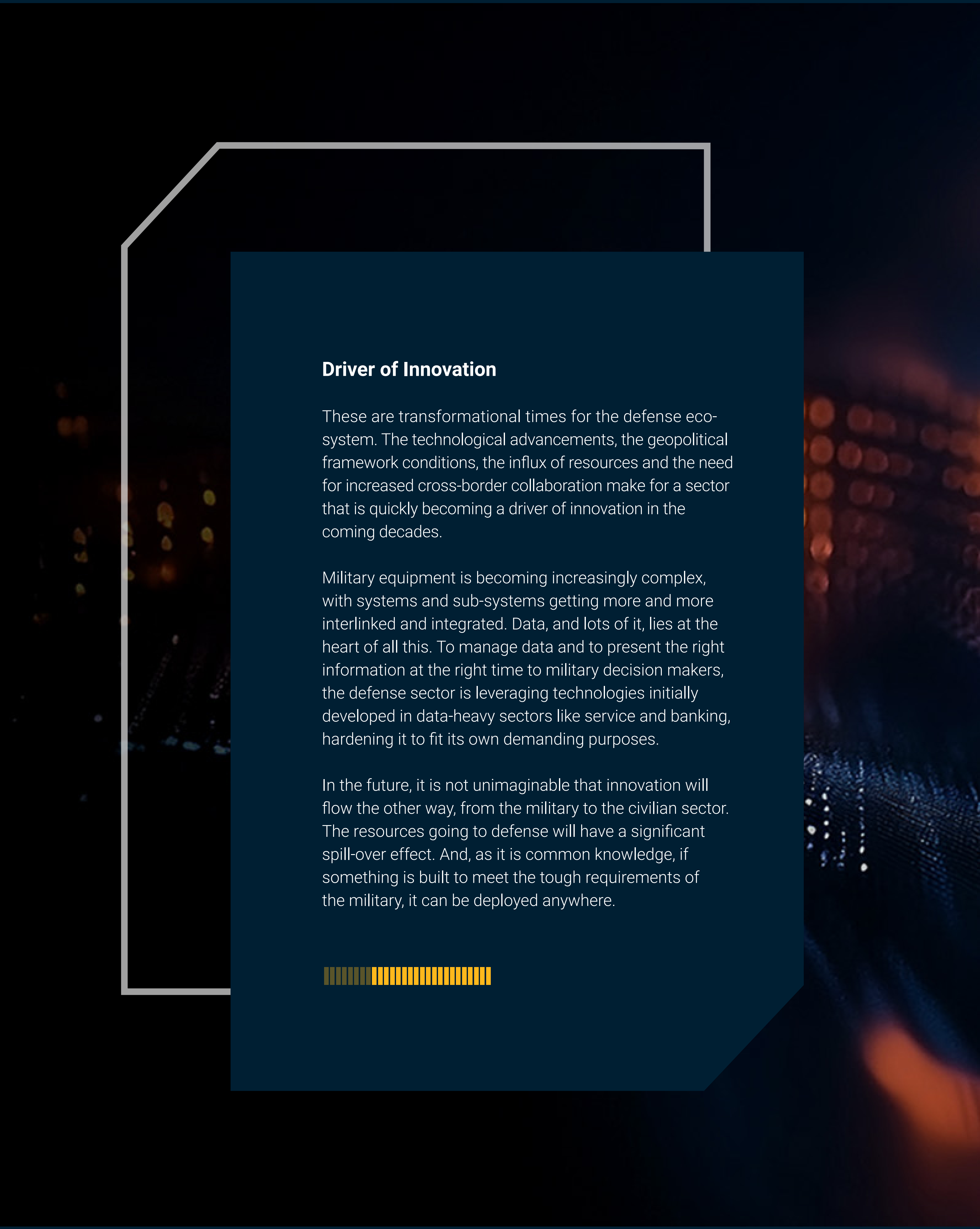
At the same time, the line between electronic warfare and cyber operations is disappearing. The same systems used to jam communications can now deliver malware, and the same techniques used to spoof GPS signals can compromise navigation systems.

And defenders are responding. Zero-trust architectures are moving from enterprise networks to tactical systems. The principle is simple: never trust, always verify. Every user, device, and data flow must be authenticated and authorized, regardless of location.

AI-driven threat detection is being pushed to the edge. Systems can now identify anomalous behavior and potential intrusions without constant connectivity to central security operations centers.

Resilient communications networks are being developed that can detect tampering or compromise and automatically reroute through secure channels.

Secure-by-design hardware is becoming a priority, with tamper-resistant components and built-in encryption that doesn't rely on software that could be compromised.



Driver of Innovation

These are transformational times for the defense eco-system. The technological advancements, the geopolitical framework conditions, the influx of resources and the need for increased cross-border collaboration make for a sector that is quickly becoming a driver of innovation in the coming decades.

Military equipment is becoming increasingly complex, with systems and sub-systems getting more and more interlinked and integrated. Data, and lots of it, lies at the heart of all this. To manage data and to present the right information at the right time to military decision makers, the defense sector is leveraging technologies initially developed in data-heavy sectors like service and banking, hardening it to fit its own demanding purposes.

In the future, it is not unimaginable that innovation will flow the other way, from the military to the civilian sector. The resources going to defense will have a significant spill-over effect. And, as it is common knowledge, if something is built to meet the tough requirements of the military, it can be deployed anywhere.

AKKODIS

Engineering a Smarter Future Together.

Contacts

United Kingdom

Vincent Bouniort

Key Accounts Manager, Defense
E: vincent.bouniort@akkodis.com

Global

Sylvain Oudinet

VP – Global Industry Director Defense & Space
E: sylvain.oudinet@akkodis.com

Italy

Alessandro Massei

Head of Sector – Aerospace, Defense, Railway
E: alessandro.massei@akkodis.com

Nordics

Fredrik Landberg

VP Defense Akkodis Group Nordics
E: flb@akkodis.se

Germany

Tobias Saathoff

Business Unit Manager Defense
E: tobias.saathoff@akkodis.com

Spain

Laura de la Cruz

Aerospace & Defense Division Director
E: laura.delacruz@akkodis.com

France

Mikael Marsal

Key Accounts Manager, Defense
E: mikael.marsal@akkodis.com

akkodis.com